IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

THE PACID GROUP, LLC,	§	
	§	
Plaintiff,	§	
	§	
v.	§	**CIVIL ACTION No. 6:09cv143-LED-JDL**
	§	
APPLE, INC., ET AL.,	§	
	§	
Defendants.	§	

ORDER

This provisional claim construction Order sets forth the Court's initial construction for the disputed claim terms in the patents asserted by Plaintiff The PACid Group, LLC ("PACid"). PACid asserts U.S. Patent Nos. 5,963,646 ("the '646 patent") and 6,049,612 ("the '612 patent") and has filed an Opening Claim Construction Brief (Doc. No. 251) ("Opening"), as well as a Reply in support of PACid's proposed constructions (Doc. No. 269) ("Reply"). Defendants Atheros Communications, Inc., Broadcom Corporation, Intel Corporation, and Marvell Semiconductor Inc. (collectively, "Defendants") have filed a Responsive Claim Construction Brief (Doc. No. 265) ("Response"). A full analysis of the disputed claim terms will be included in the Memorandum Opinion and Order, which will be issued at a later point. Despite the issuance of the instant Order, the Court may modify these initial constructions when the full Memorandum Opinion and Order is issued. The instant Order provides a guideline and framework from which to proceed at an earlier point in the litigation.

BACKGROUND

On March 30, 2009, PACid filed the instant action against Defendants, alleging infringement of the '646 and '612 patents. (Doc. No. 1). A *Markman* hearing was held on March

25, 2010 (Doc. No. 285), where thirteen disputed claim terms or "groups" of claim terms were

submitted to the Court for construction. (Doc. No. 273-1) ("Joint Chart").[1]

DISCUSSION

The Court construes the following disputed claim terms: 1) "pseudo-random," 2) "constant

value" 3) "shuffled bit result" and its relevant permutations,[2] 4) "secure hash operation" and its

relevant permutations,[3] 5) "performing a secure hash operation on said shuffled bit result to produce

a message digest," 6) "performing a secure hash operation on said first pseudo-random result to

 . . . produce a second pseudo-random result," 7) "algebraic function," 8) "host system," 9) "logic

function," 10) "cryptographic function," 11) "information file" or "message file," 12)

"concatenating," and 13) "interrupt control means."[4]

I.   "pseudo-random"[5]

Plaintiff's Proposed Construction	Defendants' Proposed Construction
No construction necessary; alternatively, "apparently random, but repeatable and predictable"	"refers to output that is repeatable and predictable to anyone who knows the function's input but appears to be totally random to those without such knowledge"

---

[1] The parties provided the Joint Claim Chart pursuant to P.R. 4-5(d).

[2] These permutations include: "bit shuffling operations," "bit shuffling function," "function to shuffle bits," and "bit shuffle computer program."

[3] These permutations include: "secure hash computer program" and "secure hash algorithm."

[4] The parties have also agreed to a number of constructions. *See* JOINT CHART.

[5] The term "pseudo-random" is contained in claims 1, 12, 17, and 26 of the '646 patent and claim 1 of the '612 patent.

The Court finds that the proper construction of the term "pseudo-random" is "refers to output that is repeatable and predictable to anyone who knows the function's input but appears to be totally random to those without such knowledge."

II.   "constant value"[6]

Plaintiff's Proposed Construction	Defendants' Proposed Construction
No construction necessary; alternatively, "a value that does not change for any given instance of generating an encryption key"	"a value that does not change"

The Court finds that "constant value" means "a value that does not change." While the construction of this term will be fully addressed in the *Markman* Opinion, the Court preliminarily notes that under this construction: different encryption keys may be produced using different constant values; and the same constant value (value that does not change) is employed when repeatedly producing a particular encryption key.

III.   "shuffled bit result" and its relevant permutations

Permutation of Claim Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
"shuffled bit result"[7]	"the result of an operation that mixes the bits of its inputs"	"the result of an operation that mixes and maps the bits of its inputs"

---

[6] The term "constant value" is contained in claims 1, 6, and 12–16 of the '646 patent and claims 1 and 7 of the '612 patent.

[7] The term "shuffled bit result" is contained in claims 1, 3, 18 of the '646 patent.

"bit shuffling operations"[8]	No separate construction (in light of the others); alternatively, "operations that mix the bits of inputs"	"operations that mixes and maps the bits of their inputs"
"bit shuffling function"[9]	No separate construction (in light of the others); alternatively, "a function that mixes the bits of its inputs"	"a function that mixes and maps the bits of its inputs"
"function to shuffle bits"[10]	No separate construction (in light of the others); alternatively, "a function that mixes the bits of its inputs"	"a function that mixes and maps the bits of its inputs"
"bit shuffle computer program"[11]	No separate construction (in light of the others); alternatively, "a computer program that mixes the bits of its inputs"	"computer program that performs a bit shuffle operation"

The Court finds that the proper construction of the term "shuffled bit result" is "the result of an operation that mixes the bits of its inputs."

The construction of the term "bit shuffling operations" is "operations that mix the bits of inputs."

---

[8] The term "bit shuffling operations" is contained in claim 18 of the '646 patent.

[9] The term "bit shuffling function" is contained in claim 19 of the '646 patent.

[10] The term "function to shuffle bits" is contained in claim 1 of the '612 patent.

[11] The term "bit shuffle computer program" is contained in claim 12 of the '646 patent.

The construction of the terms "bit shuffling function" and "function to shuffle bits" is "a function that mixes the bits of its inputs."

The construction of the term "bit shuffle computer program" is "a computer program that mixes the bits of its inputs."

IV.   "secure hash operation" and its relevant permutations

ermutation of Claim Term	Plaintiff's Proposed Construction	Defendants' Proposed Construction
"secure hash operation"[12]	"algorithm that produces a deterministic output having no known relationship with the input that may be used to recover the input from the output"	"an operation that accepts an input that can be of variable bit length, but always produces an output having the same bit length such that it is computationally infeasible to determine (a) the input from the output and (b) two inputs that produce the same output, and where if a single bit of the input is changed, on average approximately 50% of the output bits are changed"
"secure hash algorithm"[13]	"algorithm that produces a deterministic output having no known relationship with the input that may be used to recover the input from the output"	"an algorithm that accepts an input that can be of variable bit length, but always produces an output having the same bit length such that it is computationally infeasible to determine (a) the input from the output and (b) two inputs that produce the same output, and where if a single bit of the input is changed, on average approximately 50% of the output bits are changed"

---

[12] The term "secure hash operation" is contained in claim 1 of the '646 patent and claim 1 of the '612 patent.

[13] The term "secure hash algorithm" is contained in claim 12 of the '646 patent.

"secure hash computer program"[14]	No separate construction (in light of the others); alternatively, "a computer program that produces a deterministic output having no known relationship with the input that may be used to recover the input from the output"	"computer program that uses a secure hash algorithm" (as defined above)

The Court finds that the proper construction for "secure hash operation" is "a deterministic operation that produces a fixed output bit length regardless of input bit length such that it is practically impossible to determine (a) the input from the output, and (b) two inputs from the same output and where if a single bit of the input is changed, on average at least approximately 50% of the output bits are changed."

The Court finds that the proper construction of "secure hash algorithm" is "an algorithm that implements a secure hash operation."

The Court finds that the proper construction of "secure has computer program" is "a computer program that implements a secure hash operation."

---

[14] The term "secure hash computer program" is contained in claim 12 of the '646 patent.

V.   "performing a secure hash operation on said shuffled bit result to produce a message digest"[15]

Plaintiff's Proposed Construction	Defendants' Proposed Construction
No separate construction (in light of the others)	"the input to the secure hash operation is the shuffled bit result from step (a), and the output of the secure hash operation is a message digest"

The Court finds that the term "performing a secure hash operation on said shuffled bit result to produce a message digest" does not need additional construction in light of the other constructions provided herein. The scope of this claim term will be addressed in the full *Markman* Opinion.

VI.   "performing a secure hash operation on said first pseudo-random result to . . . produce a second pseudo-random result"[16]

Plaintiff's Proposed Construction	Defendants' Proposed Construction
No separate construction (in light of the others); alternatively, "performing an algorithm that produces a deterministic output having no known relationship with the input that may be used to recover the input from the output"	"the input to the secure hash operation . . . is the first pseudo-random result from step (a) and the output of the secure hash operation is a second pseudo-random result"

The Court finds that the term "performing a secure hash operation on said first pseudo-random result to . . . produce a second pseudo-random result" does not need additional

---

[15] The term "performing a secure hash operation on said shuffled bit result to produce a message digest" is contained in claim 1 of the '646 patent.

[16] The term "performing a secure hash operation on said first pseudo-random result to. . . produce a second pseudorandom result" is contained in claim 1 of the '612 patent.

construction in light of the other constructions provided herein. The scope of this claim term will

be addressed in the full *Markman* Opinion.

VII.   "algebraic function"[17]

Plaintiff's Proposed Construction	Defendants' Proposed Construction
No construction necessary; alternatively, "any operation used in mathematics"	"any operation used in mathematics or logic"

The Court finds that the proper construction of the term "algebraic function" is "any

operation used in mathematics or logic."

VIII.   "host system"[18]

Plaintiff's Proposed Construction	Defendants' Proposed Construction
No construction necessary; alternatively, "a system for providing command sequences"	"computer that inputs command sequences to an encryption key generator"

The Court finds that the proper construction of the term "host system" is "a computer that

provides command sequences through an I/O interface." While the construction of this term will

be fully addressed in the full *Markman* Opinion, the Court preliminarily notes that the word

"computer" is used in a broad sense as an intelligent computing resource and is not limited to a

typical box computer or to the entire contents of a box computer. *E.g.*, *Soverain Software LLC v.*

Amazon.com, Inc., No. 6:04-CV-14, 2005 WL 6225276, at *9 (E.D. Tex. Apr. 7, 2005) (defining

---

[17] The term "algebraic function" is contained in claims 3, 13, and 16 of the '646 patent and claims 1 and 3 of the '612 patent.

[18] The term "host system" is contained in claim 12 of the '646 patent.

"computer" to mean, "a functional unit that can perform substantial computation, including numerous arithmetic operations, or logic operations without human intervention.").

IX.   "logic function"[19]

Plaintiff's Proposed Construction	Defendants' Proposed Construction
No construction necessary; alternatively, "a function involving operations on variables that may only take a finite number of possible values or states"	"a function that involves yes-no decisions"

The Court finds that the proper construction of the term "logic function" is "a function involving operations on variables that may only take a finite number of possible values or states." It is additionally noted that this construction was agreed to by the parties prior to the *Markman* hearing. *See* JOINT CHART at x; RESPONSE at 25 ("In order to narrow the issues now at hand, Defendants agree to PACid's alternative proposed construction of this term."). Accordingly, the Court will not address this term in the full *Markman* Opinion.

X.   "cryptographic function"[20]

Plaintiff's Proposed Construction	Defendants' Proposed Construction
No construction necessary; alternatively, "a function used in encoding or decoding"	"a function used in encryption or decryption"

The Court finds that the proper construction of the term "cryptographic function" is "a function used in encoding and decoding, including encryption or decryption." It is additionally

---

[19] The term "logic function" is contained in claims 14 and 16 of the '646 patent and claim 4 of the '612 patent.

[20] The term "cryptographic function" is contained in claim 15 of the '646 patent and claim 5 of the '612 patent.

noted that this construction was agreed to by the parties prior to the *Markman* hearing. *See* JOINT

CHART at x; RESPONSE at 25 ("Defendants agree with PACid that 'cryptographic function' should

be construed broadly to encompass any function that can be used in encoding/encrypting or

decoding/decrypting. Based on the clarification in PACid's brief that encoding encompasses

encrypting and decoding encompasses decrypting, Defendants can now agree to PACid's

alternative proposed construction: 'a function used in encoding or decoding.'"). Accordingly, the

Court will not address this term in the full *Markman* Opinion.

XI. "information file" or "message file"[21]

Plaintiff's Proposed Construction	Defendants' Proposed Construction
"message or file"	"a collection of information stored as a unit and identified by a unique name"

The Court finds that the proper construction of the term "information file" is "an organized

collection of information that can be assessed and manipulated as a single named unit." Similarly,

the proper construction for "message file" is "a message that can be assessed and manipulated as

a single named unit."

XII. "concatenating"[22]

Plaintiff's Proposed Construction	Defendants' Proposed Construction
No construction necessary; alternatively, "linking units together"	"placing one bit field directly next to another"

---

[21] The term "information file" is contained in claim 1 of the '612 patent.

[22] The term "concatenating" is contained in claim 1 of the '612 patent.

The Court finds that the proper construction of the term "concatenating" is "placing one bit field side-by-side with another." While the construction of this term will be fully addressed in the full *Markman* Opinion, the Court preliminarily notes that under the Court's construction, the bit fields need not be directly next to each other as long as they are part of a group of side-by-side fields.

XIII.   "interrupt control means"[23]

Plaintiff's Proposed Construction	Defendants' Proposed Construction
Section 112(6) does not apply and no construction is necessary; alternatively: "hardware or software that issues a signal to interrupt the operation of a processor" 112(6) Function: issuing an interrupt signal upon receipt of command sequences Corresponding Structure: interrupt control unit 104	Section 112(6) applies. 112(6) Function: issuing an interrupt signal upon receipt of said command sequences Corresponding Structure: None; claim is indefinite.

The Court finds that Section 112(6) applies, and the Court will construe "interrupt control means" as a means-plus-function term. The parties agree that the function is "issuing an interrupt signal upon receipt of command sequences." The parties dispute the corresponding structure to perform the claimed function, but the Court finds that the proper function is "interrupt control unit 104," as disclosed in the '646 patent specification at 6:43–7:6; 8:3–13; and Fig. 3.

---

[23] The term "interrupt control means" is contained in claims 12 and 26 of the '646 patent. Defendants assert that this claim term is indefinite. *See* Doc. No. 264. The Court will additionally address "interrupt control means" in a separate Report and Recommendation to issue at a later time.

CONCLUSION

The Court sets forth the foregoing construction on a provisional basis. The Court may modify this provisional construction when a full Memorandum Opinion and Order on the disputed claim construction terms is issued. For the ease of reference, the Court's claim interpretations are set forth in a table attached to this Order as Appendix A.

So ORDERED and SIGNED this 21st day of April, 2010.

_____
JOHN D. LOVE
UNITED STATES MAGISTRATE JUDGE

IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF TEXAS
TYLER DIVISION

THE PACID GROUP, LLC,	§	
	§	
Plaintiff,	§	
	§	
v.	§	**CIVIL ACTION No. 6:09cv143-LED-JDL**
	§	
APPLE, INC., ET AL.,	§	
	§	
Defendants.	§	

APPENDIX A

U.S. PATENT Nos. 5,963,646 and 6,049,612

Claim Language	Patent	Claims	Plaintiff's Proposed Construction	Defendants' Proposed Construction	Court's Construction
"pseudo-random"	'646 patent '612 patent	claims 1, 12, 17, and 26 claim 1	No construction necessary; alternatively, "apparently random, but repeatable and predictable"	"refers to output that is repeatable and predictable to anyone who knows the function's input but appears to be totally random to those without such knowledge"	"refers to output that is repeatable and predictable to anyone who knows the function's input but appears to be totally random to those without such knowledge"
"constant value"	'646 patent '612 patent	claims 1, 6, and 12–16 claims 1 and 7	No construction necessary; alternatively, "a value that does not change for any given instance of generating an encryption key"	"a value that does not change"	"a value that does not change"
"shuffled bit result"	'646 patent	claims 1, 3, and 18	"the result of an operation that mixes the bits of its inputs"	"the result of an operation that mixes and maps the bits of its inputs"	"the result of an operation that mixes the bits of its inputs"
"bit shuffling operations"	'646 patent	claim 18	No separate construction (in light of the others); alternatively, "operations that mix the bits of inputs"	"operations that mixes and maps the bits of their inputs"	"operations that mix the bits of inputs"

Claim Language	Patent	Claims	Plaintiff's Proposed Construction	Defendants' Proposed Construction	Court's Construction
"bit shuffling function"	'646 patent	claim 19	No separate construction (in light of the others); alternatively, "a function that mixes the bits of its inputs"	"a function that mixes and maps the bits of its inputs"	"a function that mixes the bits of its inputs"
"function to shuffle bits"	'612 patent	claim 1	No separate construction (in light of the others); alternatively, "a function that mixes the bits of its inputs"	"a function that mixes and maps the bits of its inputs"	"a function that mixes the bits of its inputs"
"bit shuffle computer program"	'646 patent	claim 12	No separate construction (in light of the others); alternatively, "a computer program that mixes the bits of its inputs"	"computer program that performs a bit shuffle operation"	"a computer program that mixes the bits of its inputs"
"secure hash operation"	'646 patent '612 patent	claim 1 claim 1	"algorithm that produces a deterministic output having no known relationship with the input that may be used to recover the input from the output"	"an operation that accepts an input that can be of variable bit length, but always produces an output having the same bit length such that it is computationally infeasible to determine (a) the input from the output and (b) two inputs that produce the same output, and where if a single bit of the input is changed, on average approximately 50% of the output bits are changed"	"a deterministic operation that produces a fixed output bit length regardless of input bit length such that it is practically impossible to determine (a) the input from the output, and (b) two inputs from the same output and where if a single bit of the input is changed, on average at least approximately 50% of the output bits are changed"

15

Claim Language	Patent	Claims	Plaintiff's Proposed Construction	Defendants' Proposed Construction	Court's Construction
"secure hash algorithm"	'646 patent	claim 12	"algorithm that produces a deterministic output having no known relationship with the input that may be used to recover the input from the output"	"an algorithm that accepts an input that can be of variable bit length, but always produces an output having the same bit length such that it is computationally infeasible to determine (a) the input from the output and (b) two inputs that produce the same output, and where if a single bit of the input is changed, on average approximately 50% of the output bits are changed"	"an algorithm that implements a secure hash operation"
"secure hash computer program"	'646 patent	claim 12	No separate construction (in light of the others);\n\nalternatively, "a computer program that produces a deterministic output having no known relationship with the input that may be used to recover the input from the output"	"computer program that uses a secure hash algorithm" (as defined above)	"a computer program that implements a secure hash operation"
"performing a secure hash operation on said shuffled bit result to produce a message digest"	'646 patent	claim 1	No separate construction (in light of the others)	"the input to the secure hash operation is the shuffled bit result from step (a), and the output of the secure hash operation is a message digest"	No separate construction.

16

Claim Language	Patent	Claims	Plaintiff's Proposed Construction	Defendants' Proposed Construction	Court's Construction
"performing a secure hash operation on said first pseudo-random result to . . . produce a second pseudorandom result"	'612 patent	claim 1	No separate construction (in light of the others); alternatively, "performing an algorithm that produces a deterministic output having no known relationship with the input that may be used to recover the input from the output"	"the input to the secure hash operation . . . is the first pseudo-random result from step (a) and the output of the secure hash operation is a second pseudo-random result"	No separate construction.
"algebraic function"	'646 patent '612 patent	claims 3, 13, and 16 claims 1 and 3	No construction necessary; alternatively, "any operation used in mathematics"	"any operation used in mathematics or logic"	"any operation used in mathematics or logic"
"host system"	'646 patent	claim 12	No construction necessary; alternatively, "a system for providing command sequences"	"computer that inputs command sequences to an encryption key generator"	"a computer that provides command sequences through an I/O interface"
"logic function"	'646 patent '612 patent	claims 14 and 16 claim 4	No construction necessary; alternatively, "a function involving operations on variables that may only take a finite number of possible values or states"	"a function that involves yes-no decisions"	"a function involving operations on variables that may only take a finite number of possible values or states"
"cryptographic function"	'646 patent '612 patent	claim 15 claim 5	No construction necessary; alternatively, "a function used in encoding or decoding"	"a function used in encryption or decryption"	"a function used in encoding and decoding, including encryption or decryption."

Claim Language	Patent	Claims	Plaintiff's Proposed Construction	Defendants' Proposed Construction	Court's Construction
"information file" or "message file"	'612 patent	claim 1	"message or file"	"a collection of information stored as a unit and identified by a unique name"	Information file means "an organized collection of information that can be assessed and manipulated as a single named unit" Message file means "a message that can be assessed and manipulated as a single named unit"
"concatenating"	'612 patent	claim 1	No construction necessary; alternatively, "linking units together"	"placing one bit field directly next to another"	"placing one bit field side-by-side with another"
"interrupt control means"	'646 patent	claims 12 and 26	Section 112(6) does not apply and no construction is necessary; alternatively: "hardware or software that issues a signal to interrupt the operation of a processor" 112(6) Function: issuing an interrupt signal upon receipt of command sequences Corresponding Structure: interrupt control unit 104	Section 112(6) applies. 112(6) Function: issuing an interrupt signal upon receipt of said command sequences Corresponding Structure: None; claim is indefinite	Section 112(6) applies. 112(6) Function: issuing an interrupt signal upon receipt of command sequences Corresponding Structure: interrupt control unit 104